Nonbinary Quantum Reed-Muller Codes

Pradeep K. Sarvepalli
Dept. of Computer Science
Texas A&M University
College Station, TX 77843-3112, USA
Email: pradeep@cs.tamu.edu

Andreas Klappenecker
Dept. of Computer Science
Texas A&M University
College Station, TX 77843-3112, USA
Email: klappi@cs.tamu.edu

***Abstract*— We construct nonbinary quantum codes from classical generalized Reed-Muller codes and derive the conditions under which these quantum codes can be punctured. We provide a partial answer to a question raised by Grassl, Beth and Rötteler on the existence of q-ary quantum MDS codes of length n with $q \leq n \leq q^2 - 1$.**

I. Introduction

The quest to build a scalable quantum computer that is resilient against decoherence errors and operational noise has sparked a lot of interest in quantum error-correcting codes. The early research has been confined to the study of binary quantum error-correcting codes, but more recently the theory was extended to nonbinary codes that are useful in the realization of fault-tolerant computations.

The purpose of this paper is to derive families of quantum stabilizer codes that are based on classical generalized Reed-Muller (GRM) codes. Recall that one cannot arbitrarily shorten a quantum stabilizer code. We study the puncture codes of GRM stabilizer codes that determine the possible lengths of shortened codes.

We give now an overview of our main theorems. We omit some technical details to keep our exposition brief, but we assure the reader that the subsequent sections provide all missing details. Let q be power of a prime. We denote by $\mathcal{R}_q(\nu, m)$ the q-ary generalized Reed-Muller code of order ν with parameters $[q^m, k(\nu), d(\nu)]_q$ and dual distance $d(\nu^\perp)$.

Our first two results concern the construction of two families of nonbinary quantum stabilizer codes:

Theorem 1: For $0 \leq \nu_1 \leq \nu_2 \leq m(q-1) - 1$, there exist pure quantum stabilizer codes with the parameters $[[q^m, k(\nu_2) - k(\nu_1), \min\{d(\nu_1^\perp), d(\nu_2)\}]]_q$.

Theorem 2: For $0 \leq \nu \leq m(q-1) - 1$, there exists a pure $[[q^{2m}, q^{2m} - 2k(\nu), d(\nu^\perp)]]_q$ quantum stabilizer code.

Puncturing a quantum stabilizer code is restricted because the underlying classical code must remain self-orthogonal. Our next two results show when quantum Reed-Muller codes can be punctured.

Theorem 3: For $0 \leq \nu_1 \leq \nu_2 \leq m(q-1) - 1$ and $0 \leq \mu \leq \nu_2 - \nu_1$, if $\mathcal{R}_q(\mu, m)$ has a codeword of weight r, then there exists an $[[r, \geq (k(\nu_2) - k(\nu_1) - q^m + r), \geq d]]_q$ quantum stabilizer code with $d = \min\{d(\nu_2), d(\nu_1^\perp)\}$.

Theorem 4: Let $C = \mathcal{R}_{q^2}(\nu, m)$ with $0 \leq \nu \leq m(q-1) - 1$ and $(q+1)\nu \leq \mu \leq m(q^2-1)-1$. If $\mathcal{R}_{q^2}(\mu, m)^\perp|_{\mathbf{F}_q}$ contains a vector of weight r, then there exists a quantum stabilizer code with parameters $[[r, \geq (r - 2k(\nu)), \geq d(\nu^\perp)]]_q$.

Our last result deals with the existence of quantum MDS codes of length n with $q \leq n \leq q^2 - 1$. These are derived from the previous results on punctured codes making use of some additional properties of MDS codes.

Theorem 5: There exist quantum MDS codes with the parameters $[[(\nu+1)q, (\nu+1)q - 2\nu - 2, \nu+2]]_q$ for $0 \leq \nu \leq q-2$.

The paper is organized as follows. In the next section we review the basics of generalized Reed-Muller codes. We construct two series of quantum codes using a nonbinary version of the CSS construction and a Hermitian construction. In Section III, we derive our results concerning the puncturing of these stabilizer codes. In Section IV, we consider a special case of GRM codes to obtain some quantum MDS codes. The MDS nature of these codes allows us to make some more definitive statements about their puncture codes, making it possible to show the existence of quantum MDS codes of lengths between q and q^2.

Notation: We denote the Euclidean inner product of two vectors x and y in $\mathbf{F}_q^n$ by $\langle x|y \rangle = x_1 y_1 + \cdots x_n y_n$. We write $\langle x|y \rangle_h = x_1 y_1^q + \cdots x_n y_n^q$ to denote the Hermitian inner product of two vectors x and y in $\mathbf{F}_{q^2}^n$. We denote the Euclidean dual of a code $C \subseteq \mathbf{F}_q^n$ by $C^\perp$, and the Hermitian dual of a code $D \subseteq \mathbf{F}_{q^2}^n$ by $D^{\perp_h}$.

II. Generalized Reed-Muller Codes

Primitive generalized Reed-Muller codes were introduced by Kasami, Lin, and Petersen [8] as a generalization of Reed-Muller codes [10], [13]. We follow Assmus and Key [2], [3] in our approach to GRM codes. Our main goal is to derive two series of quantum stabilizer codes.

A. Classical Codes

Let $(P_1, \ldots, P_n)$ denote an enumeration of all points in $\mathbf{F}_q^m$ with $n = q^m$. We denote by $L_m(\nu)$ the subspace of $\mathbf{F}_q[x_1, \ldots, x_m]$ that is generated by polynomials of degree ν or less. Let ν denote an integer in the range $0 \leq \nu < m(q-1)$. Let ev denote the evaluation function $ev\ f = (f(P_1), \ldots, f(P_n))$. The generalized Reed-Muller code $\mathcal{R}_q(\nu, m)$ of order ν is defined as

$$\begin{aligned} \mathcal{R}_q(\nu, m) &= \{(f(P_1), \ldots, f(P_n)) \mid f \in L_m(\nu)\}, \quad (1) \\ &= \{ev\ f \mid f \in L_m(\nu)\}. \end{aligned}$$

The dimension $k(\nu)$ of the code $\mathcal{R}_q(\nu,m)$ equals

$$k(\nu) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m+\nu-jq}{\nu-jq}, \quad (2)$$

and its minimum distance $d(\nu)$ is given by

$$d(\nu) = (R+1)q^Q, \quad (3)$$

where $m(q-1)-\nu = (q-1)Q+R$, such that $0 \leq R < q-1$; see [2], [3], [8], [11].

It is clear that $\mathcal{R}_q(\nu,m) \subseteq \mathcal{R}_q(\nu',m)$ holds for all parameters $\nu \leq \nu'$. More interesting is the fact that the dual code of $\mathcal{R}_q(\nu,m)$ is again a generalized Reed-Muller code,

$$\mathcal{R}_q(\nu,m)^\perp = \mathcal{R}(\nu^\perp,m) \quad \text{with} \quad \nu^\perp = m(q-1)-1-\nu.$$

We need the following result for determining the distances and purity of quantum codes.

Lemma 1: Let $C_1 = \mathcal{R}_q(\nu_1,m)$ and $C_2 = \mathcal{R}_q(\nu_2,m)$. If $v_1 < v_2$, then $C_1 \subset C_2$ and $\mathrm{wt}(C_2 \setminus C_1) = \mathrm{wt}(C_2)$.

Proof: We already know that $C_1 \subset C_2$ if $\nu_1 < \nu_2$. We denote the minimum distances of the codes C_1 and C_2 by $d_1 = \mathrm{wt}(C_1) = (R_1+1)q^{Q_1}$ and $d_2 = \mathrm{wt}(C_2) = (R_2+1)q^{Q_2}$.

It suffices to show that $\nu_1 < \nu_2$ implies $d_2 < d_1$, because in that case $C_2 \setminus C_1$ must contain a vector of weight d_2, and this shows that $\mathrm{wt}(C_2 \setminus C_1) = \mathrm{wt}(C_2)$, as claimed.

Since $\nu_1 < \nu_2$, we have

$$m(q-1)-\nu_2 < m(q-1)-\nu_1. \quad (4)$$

If we set $m(q-1)-\nu_k = (q-1)Q_k+R_k$ with $0 \leq R_k < q-1$ for $k \in \{1,2\}$, then it follows from (4) that $Q_1 \geq Q_2$.

If $Q_1 = Q_2$ then $R_1 > R_2$; hence, $d_1 = (R_1+1)q^{Q_1} > (R_2+1)q^{Q_2} = d_2$. On the other hand, if $Q_1 > Q_2$, then $d_1 \geq (0+1)q^{Q_1}$ and $d_2 \leq (q-2+1)q^{Q_2} = (q-1)q^{Q_2}$, and it follows that $d_1 \geq q^{Q_2+1} > d_2$. ■

B. Quantum codes

Quantum Reed-Muller codes were first constructed by Steane [14] based on classical Reed-Muller codes. We derive a series of stabilizer codes from generalized Reed-Muller codes using the CSS code construction and a Hermitian code construction.

Lemma 2: Let $C_1 = [n,k_1,d_1]_q$ and $C_2 = [n,k_2,d_2]_q$ be linear codes over $\mathbf{F}_q$ with $C_1 \subseteq C_2$. Furthermore, let $d = \min \mathrm{wt}\{(C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$ if $C_1 \subset C_2$ and $d = \min \mathrm{wt}\{(C_1) \cup (C_1^\perp)\}$ if $C_1 = C_2$. Then there exists an $[[n,k_2-k_1,d]]_q$ quantum code.

Proof: See for instance [4] for the CSS construction of binary codes and [6, Theorem 3] and [9] for its q-ary generalizations. ■

Theorem 1: For $0 \leq \nu_1 \leq \nu_2 \leq m(q-1)-1$, there exists a pure $[[q^m, k(\nu_2)-k(\nu_1), \min\{d(\nu_1^\perp), d(\nu_2)\}]]_q$ quantum stabilizer code, where the parameters $k(\nu)$ and $d(\nu)$ are given by the equations (2) and (3), respectively.

Proof: For $\nu_1 \leq \nu_2$, $C_1 = \mathcal{R}_q(\nu_1,m) \subseteq \mathcal{R}_q(\nu_2,m) = C_2$. By Lemma 2, we know there exists a pure $[[q^m, k(\nu_2) - k(\nu_1), \min\{d(\nu_1^\perp), d(\nu_2)\}]]_q$ quantum code. The purity of the code follows from Lemma 1. ■

Corollary 3: For $0 \leq \nu \leq (m(q-1)-1)/2$ there exists a pure $[[n, n-2k(\nu), d(\nu^\perp)]]_q$ quantum code, where $k(\nu)$ is given by equation (2) and the distance $d(\nu)$ by equation (3).

Proof: In Theorem 1 if we choose $\nu_1 = \nu$, $\nu_2 = \nu^\perp$, then to ensure $\nu_1 \leq \nu_2$ we require $\nu \leq (m(q-1)-1)/2$. That the distance of the resulting code is $d(\nu^\perp)$ follows by direct substitution of these values in Theorem 1. ■

The next construction starts from a generalized Reed-Muller code over $\mathbf{F}_{q^2}$. If it is contained in its Hermitian dual code, then it can be used to construct quantum codes. Therefore, our immediate goal will be to find such self-orthogonal Reed-Muller codes.

Lemma 4: If ν is an order in the range $0 \leq \nu \leq m(q-1)-1$, then $\mathcal{R}_{q^2}(\nu,m) \subseteq \mathcal{R}_{q^2}(\nu,m)^{\perp_h}$.

Proof: Recall that $ev\, f = (f(P_1), \dots, f(P_n))$. The code $\mathcal{R}_{q^2}(0,m)$ is generated by $\mathbf{1}$, the all one vector. The relation $\mathcal{R}_{q^2}(0,m)^\perp = \mathcal{R}_{q^2}(m(q^2-1)-1,m)$ shows that $\langle ev\, f | \mathbf{1} \rangle = 0$ for all polynomials f in $L_m(\nu)$ with $\deg f \leq m(q^2-1)-1$. If $x_1^{a_1} \cdots x_m^{a_m}$ and $x_1^{b_1} \cdots x_m^{b_m}$ are monomials in $L_m(\nu)$, then

$$\begin{aligned} &\langle ev\, x_1^{a_1} \cdots x_m^{a_m} \mid ev\, x_1^{b_1} \cdots x_m^{b_m} \rangle_h \\ &\quad = \langle ev\, x_1^{a_1} \cdots x_m^{a_m} \mid ev\, x_1^{qb_1} \cdots x_m^{qb_m} \rangle, \\ &\quad = \langle ev\, x_1^{a_1+qb_1} \cdots x_m^{a_m+qb_m} \mid \mathbf{1} \rangle = 0, \end{aligned}$$

where the last equality holds because the monomial has at most degree $(m(q-1)-1)(q+1) < m(q^2-1)-1$. Since the monomials generate $L_m(\nu)$, it follows that $\langle ev\, f | \, ev\, g \rangle_h = 0$ for all f, g in $L_m(\nu)$. ■

The following construction, which we refer to as the Hermitian construction, directly leads to the second series of quantum codes that can be constructed from the Reed-Muller codes.

Lemma 5: Let C be a linear $[n,k]_{q^2}$ contained in its Hermitian dual, $C^{\perp_h}$, such that $d = \min\{\mathrm{wt}(C^{\perp_h} \setminus C)\}$. Then there exists an $[[n, n-2k, d]]_q$ quantum code.

Proof: See for instance [1, Corollary 1] and [6, Corollary 2]. ■

Theorem 2: For $0 \leq \nu \leq m(q-1)-1$, there exist pure quantum codes $[[q^{2m}, q^{2m}-2k(\nu), d(\nu^\perp)]]_q$, where

$$k(\nu) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m+\nu-jq^2}{\nu-jq^2},$$

and $d(\nu^\perp) = (R+1)q^{2Q}$, with $\nu+1 = (q^2-1)Q+R$ and $0 \leq R < q^2-1$.

Proof: First we note that $\mathrm{wt}(\mathcal{R}_{q^2}(\nu,m)^{\perp_h}) = \mathrm{wt}(\mathcal{R}_{q^2}(\nu,m)^\perp) = d(\nu^\perp)$. Recall that $d(\nu^\perp)$ can be computed using equation (3), keeping in mind that these codes are over $\mathbf{F}_{q^2}$. From Lemma 4 and Lemma 5 we can conclude that there exists a pure quantum code $[[q^{2m}, q^{2m}-2k(\nu), d(\nu^\perp)]]_q$ where $k(\nu)$ is the dimension of $\mathcal{R}_{q^2}(\nu,m)$ as given by equation (2). The purity of the code follows from Lemma 1. ■

III. Puncturing Quantum GRM Codes

Puncturing provides a means to construct new codes from existing codes. Puncturing quantum stabilizer codes, however, is not as straightforward as in the case of classical codes. Rains introduced the notion of puncture code [12], which simplified this problem and provided a means to find out when punctured codes are possible. Further extensions to these ideas can be found in [6]. With the help of these results we now study the puncturing of GRM codes.

Recall that for every quantum code constructed using the CSS construction, we can associate two classical codes, C_1 and C_2. Define C to be the direct sum of C_1 and $C_2^\perp$ viz. $C = C_1 \oplus C_2^\perp$. The puncture code $P(C)$ [6, Theorem 12] is defined as

$$P(C) \quad = \quad \{(a_i b_i)_{i=1}^n \mid a \in C_1, b \in C_2^\perp\}^\perp. \tag{5}$$

The usefulness of the puncture codes lies in the fact that if there exists a vector of nonzero weight r, then the corresponding quantum code can be punctured to a length r and minimum distance greater than or equal to distance of the parent code.

Theorem 3: For $0 \le \nu_1 \le \nu_2 \le m(q-1)-1$ and $0 \le \mu \le \nu_2 - \nu_1$, if $\mathcal{R}_q(\mu, m)$ has codeword of weight r, then there exists an $[[r, \ge (k(\nu_2)-k(\nu_1)-q^m+r), \ge d]]_q$ quantum code, where $d = \min\{d(\nu_2), d(\nu_1^\perp)\}$. In particular, there exists a $[[d(\mu), \ge (k(\nu_2)-k(\nu_1)-q^m+d(\mu)), \ge d]]_q$ quantum code.

Proof: Let $C_i = \mathcal{R}_q(\nu_i, m)$ with $0 \le \nu_1 \le \nu_2 \le m(q-1)-1$, for $i \in \{1,2\}$. By Theorem 1, a $[[q^m, k(\nu_2)-k(\nu_1), d]]_q$ quantum code Q with $d = \min\{d(\nu_2), d(\nu_1^\perp)\}$ exists. It follows from equation (5) that $P(C)^\perp = \mathcal{R}_q(\nu_1 + \nu_2^\perp, m)$, so

$$\begin{aligned} P(C) &= \mathcal{R}_q(m(q-1) - \nu_1 - \nu_2^\perp - 1, m) \\ &= \mathcal{R}_q(\nu_2 - \nu_1, m) \end{aligned} \tag{6}$$

By [6, Theorem 11], if there exists a vector of weight r in $P(C)$, then there exists an $[[r, k', d']]_q$ quantum code, where $k' \ge (k(\nu_2) - k(\nu_1) - q^m + r)$ and distance $d' \ge d$. Since $P(C) = \mathcal{R}_q(\nu_2 - \nu_1, m) \supseteq \mathcal{R}_q(\mu, m)$ for all $0 \le \mu \le \nu_2 - \nu_1$, the weight distributions of $\mathcal{R}_q(\mu, m)$ give all the lengths to which Q can be punctured. Moreover $P(C)$ will certainly contain vectors whose weight $r = d(\mu)$, that is the minimum weight of $\mathcal{R}_q(\mu, m)$. Thus there exist punctured quantum codes with the parameters $[[d(\mu), \ge (k(\nu_2) - k(\nu_1) - q^m + d(\mu)), \ge d]]_q$. ∎

It is also possible to puncture codes constructed via Theorem 2. However, we need to redefine the puncture code. Recall a quantum code constructed via the Hermitian construction has an underlying classical code $C \subseteq \mathbf{F}_{q^2}^n$. The (Hermitian) puncture code, $P_h(C)$, is defined as [6, Theorem 13]

$$P_h(C) = \{\mathrm{tr}_{q^2/q}(a_i b_i^q)_{i=1}^n \mid a, b \in C\}^\perp, \tag{7}$$

where the subscript is used to differentiate the two constructions. Again the nonzero weights in the puncture code determine the possible puncturings of the quantum code. Now we shall apply these ideas to the puncturing of quantum Reed-Muller codes constructed using the Hermitian construction.

Theorem 4: Let $C = \mathcal{R}_{q^2}(\nu, m)$ with $0 \le \nu \le m(q-1)-1$ and $(q+1)\nu \le \mu \le m(q^2-1)-1$. The puncture code $P_h(C) \supseteq \mathcal{R}_{q^2}(\mu, m)^\perp|_{\mathbf{F}_q}$. If $P_h(C)$ contains a vector of weight r, then there exists an $[[r, \ge (r - 2k(\nu)), \ge d(\nu^\perp)]]_q$ quantum code[1].

Proof: By equation (7) the puncture code $P_h(C)$ is given as

$$P_h(C) = \{\mathrm{tr}_{q^2/q}(a_i b_i^q)_{i=1}^n \mid a, b \in C\}^\perp. \tag{8}$$

To get a more useful description of $P_h(C)$ let us consider the code D given by

$$D = \{(a_i b_i^q)_{i=1}^n \mid a, b \in C\}. \tag{9}$$

If $C = \mathcal{R}_{q^2}(\nu, m)$, then $a = ev\ f$ and $b = ev\ g$ for some f, g in $L_m(\nu)$. Then $a_i b_i^q = (ev\ fg^q)_i$ and we can write

$$D \quad = \quad \{ev\, fg^q \mid f, g \in L_m(\nu)\}.$$

Since deg $fg^q \le (q+1)\nu$, fg^q is in $L_m(q\nu+\nu)$ and it follows

$$\begin{aligned} D &\subseteq \{ev\, f \mid f \in L_m((q+1)\nu)\}, \\ D &\subseteq \mathcal{R}_{q^2}(\mu, m), \end{aligned} \tag{10}$$

for $(q+1)\nu \le \mu \le m(q^2-1)-1$. By Delsarte's theorem [5, Theorem 2], the dual of the trace code is the restriction of the dual code. That is,

$$\mathrm{tr}_{q^2/q}(D)^\perp \quad = \quad D^\perp|_{\mathbf{F}_q} = D^\perp \cap \mathbf{F}_q^n. \tag{11}$$

However, as $P_h(C)^\perp = \mathrm{tr}_{q^2/q}(D)$, it follows that

$$P_h(C) \quad = \quad D^\perp|_{\mathbf{F}_q} \supseteq \mathcal{R}_{q^2}(\mu, m)^\perp|_{\mathbf{F}_q}, \tag{12}$$

$$P_h(C) \quad \supseteq \quad \mathcal{R}_{q^2}(m(q^2-1) - \mu - 1, m)|_{\mathbf{F}_q} \tag{13}$$

From Theorem 2 there exists an $[[q^{2m}, q^{2m} - 2k(\nu), d(\nu^\perp)]]_q$ quantum code Q for $0 \le \nu \le m(q-1)-1$. By [6, Theorem 11], Q can be punctured to all lengths which have nonzero distribution in $P_h(C)$. Thus if $P_h(C) \supseteq \mathcal{R}_{q^2}(\mu^\perp, m)|_{\mathbf{F}_q}$ contains a vector of weight r, then there exists an $[[r, \ge (r - 2k(\nu)), \ge d(\nu^\perp)]]_q$ code. ∎

IV. Quantum MDS Codes via GRM Codes

MDS codes occupy a special place of interest in coding theory in view of their optimality with respect to the Singleton bound and also because of their many connections to other branches of mathematics. So in this section we shall construct some linear quantum MDS codes as a special case of quantum GRM codes. The usefulness of such an approach will be appreciated later when we try to puncture them.

A. Quantum MDS codes

The previous results enable us to derive very easily some qauntum MDS codes as a special case.

Corollary 6: There exist quantum MDS codes with the parameters $[[q, q-2\nu-2, \nu+2]]_q$ for $0 \le \nu \le (q-2)/2$ and $[[q^2, q^2-2\nu-2, \nu+2]]_q$ for $0 \le \nu \le q-2$.

Proof: These codes and the corresponding ranges of ν are a direct consequence of Corollary 3 and Theorem 2 with

[1] Since C is over $\mathbf{F}_{q^2}$, q^2 should be used in equations (2) and (3).

$m = 1$. In both cases it can be verified that $k(\nu) = \nu + 1$ and $d(\nu^{\perp}) = \nu + 2$. The quantum codes $[[q, q-2\nu-2, \nu+2]]_q$ and $[[q^2, q^2-2\nu-2, \nu+2]]_q$ follow on substituting the values of $k(\nu)$ and $d(\nu^{\perp})$ in these constructions. It can be easily verified that these quantum codes satisfy the quantum Singleton bound [12]. ∎

It must be noted that when applying equations (2) and (3) we must be careful to use q for Corollary 3 and q^2 for Lemma 2. An alternate approach to constructing these codes can be found in [6].

B. Puncturing Quantum MDS codes.

It was shown in [6] that there exist q-ary quantum MDS codes of lengths $3 \leq n \leq q$ as well as $q^2 - s$ for some $s > 1$. The range and the distribution of such s was not answered analytically. However numerical evidence was provided which indicated that there existed many s or equivalently many MDS codes with lengths between q and q^2. Here, we partly address this problem by analytically proving the existence of MDS codes of length $(\nu + 1)q$ with $0 \leq \nu \leq q - 2$.

We will assume that the quantum code Q is constructed using Theorem 2 and the corresponding classical code is C. As mentioned earlier, the associated puncture code $P_h(C)$ determines the lengths to which we can puncture Q (refer Theorem 4, [12, Theorem 3] and [6, Theorem 11,13]). In general it is not easy to calculate the weight distribution of $P_h(C)$, but we can simplify our task by calculating either the weight distribution or the minimum distance of a subcode in $P_h(C)$. We will need the following result proved in [11], though it is not stated explicitly as a theorem. We have restated it slightly differently to make the proofs clearer.

Lemma 7: Every GRM code $\mathcal{R}_q(\nu, m)$ is a subcode of $\mathcal{R}_{q^m}(q^m - d(\nu), 1)$. Alternatively,

$$\mathcal{R}_q(\nu, m) \subseteq \mathcal{R}_{q^m}(q^m - d(\nu), 1)|_{\mathbf{F}_q}. \tag{14}$$

Proof: See [11]. The result in [11] actually states that

$$\mathcal{R}_q(\nu, m) \subseteq GRS_{q^m - d(\nu)+1}(\mathbf{a}, \mathbf{1})|_{\mathbf{F}_q}, \tag{15}$$

where $\mathbf{a} = (0, 1, \zeta, \zeta^2, \ldots, \zeta^{q^m-2})$, ζ is a primitive element in $\mathbf{F}_{q^m}$ and $GRS_{q^m-d(\nu)+1}(\mathbf{a}, \mathbf{1})$ stands for the generalized Reed-Solomon code with the parameters $[q^m, q^m - d(\nu) + 1, d(\nu)]$ (see [7, pages 175-178]). However, as $\mathcal{R}_{q^m}(q^m - d(\nu), 1)$ is the extended Reed-Solomon code, it is the same as $GRS_{q^m-d(\nu)+1}(\mathbf{a}, \mathbf{1})$. Therefore, we can conclude that $\mathcal{R}_q(\nu, m) \subseteq \mathcal{R}_{q^m}(q^m - d(\nu), 1)|_{\mathbf{F}_q}$. ∎

Lemma 8: Let $C = \mathcal{R}_{q^2}(\nu, 1)$ with $0 \leq \nu \leq q-2$, then the puncture code $P_h(C)$ has a vector of weight $(\nu + 1)q$.

Proof: Let $C = \mathcal{R}_{q^2}(\nu, 1)$. By Theorem 4, we know that $P_h(C) \supseteq \mathcal{R}_{q^2}(\mu, 1)^{\perp}|_{\mathbf{F}_q}$, where $(q+1)\nu \leq \mu \leq (q^2 - 2)$.

$$P_h(C) \supseteq \mathcal{R}_{q^2}(\mu, 1)^{\perp}|_{\mathbf{F}_q} = \mathcal{R}_{q^2}(q^2 - \mu - 2, 1)|_{\mathbf{F}_q} \tag{16}$$

Choose $\mu = (\nu + 1)q - 2$. (Note that $(q + 1)\nu \leq (\nu + 1)q \leq q^2 - 2$ holds for $0 \leq \nu \leq q - 2$). Then

$$P_h(C) \supseteq \mathcal{R}_{q^2}(q^2 - (\nu + 1)q, 1)|_{\mathbf{F}_q}. \tag{17}$$

We will show that $\mathcal{R}_q(q - \nu - 1, 2)$ is embedded in $\mathcal{R}_{q^2}(q^2 - (\nu+1)q, 1)|_{\mathbf{F}_q}$; thus in $P_h(C)$ also. By equation (3), $\text{wt}(\mathcal{R}_q(q - \nu - 1, 2)) = d(q - \nu - 1) = (\nu + 1)q$. By Lemma 7 $\mathcal{R}_q(q - \nu - 1, 2)$ is embedded in $\mathcal{R}_{q^2}(q^2 - (\nu + 1)q, 1)|_{\mathbf{F}_q} \subseteq P_h(C)$. Hence $P_h(C)$ contains a vector of weight equal to $(\nu + 1)q$. ∎

Theorem 5: There exist quantum MDS codes with the parameters $[[(\nu+1)q, (\nu+1)q-2\nu-2, \nu+2]]_q$ for $0 \leq \nu \leq q-2$.

Proof: The puncture code of $C = \mathcal{R}_{q^2}(\nu, 1)$ has a vector of weight $(\nu+1)q$ by Lemma 8. By Theorem 4, the quantum code $[[q^2, q^2-2\nu-2, \nu+2]]_q$ derived from C can be punctured to a length of $(\nu + 1)q$, giving a code $[[(\nu + 1)q, (\nu + 1)q - 2\nu - 2, \nu + 2]]_q$ which can be verified to be a quantum MDS code. ∎

V. Conclusion

We constructed a family of nonbinary quantum codes based on the classical generalized Reed-Muller codes. Then we studied when these codes can be punctured to give more quantum codes. As a special case we derived a series of quantum MDS codes from the generalized Reed-Muller codes. We provided a partial answer to the question of existence of q-ary MDS codes with lengths in the range q to q^2 by analytically proving the existence of a series of codes with lengths in this range.

Acknowledgment

This research was supported by NSF CAREER award CCF 0347310, NSF grant CCR 0218582, a Texas A&M TITF initiative, and a TEES Select Young Faculty award.

References

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[2] A. Assmus, Jr. and J. Key, *Designs and their codes*. Cambridge: Cambridge University Press, 1992.

[3] E. Assmus, Jr. and J. Key, "Polynomial codes and finite geometries," in *Handbook of Coding Theory*, V. Pless and W. Huffman, Eds., vol. II. Amsterdam: Elsevier, 1998, pp. 1269–1343.

[4] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, 1998.

[5] P. Delsarte, "On subfield subcodes of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 21, no. 5, pp. 575–576, 1975.

[6] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Internat. J. Quantum Information*, vol. 2, no. 1, pp. 757–775, 2004.

[7] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge: University Press, 2003.

[8] T. Kasami, S. Lin, and W. W. Peterson, "New generalizations of the Reed-Muller codes Part I : Primitive codes," *IEEE Trans. Inform. Theory*, vol. 14, no. 2, pp. 189–199, 1968.

[9] J.-L. Kim and J. Walker, "Nonbinary quantum error-correcting codes from algebraic curves," submitted for publication.

[10] D. Muller, "Applications of Boolean algebra to switching circuit designand to error correction," *IRE Trans. Elec. Comp.*, vol. 3, pp. 6–12, 1954.

[11] R. Pellikaan and X.-W. Wu, "List decoding of q-ary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 4, pp. 679–682, 2004.

[12] E. Rains, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1827–1832, 1999.

[13] I. Reed, "A class of multiple-error-correcting codes and a decoding scheme," *IEEE Trans. Inform. Theory*, vol. 4, pp. 38–49, 1954.

[14] A. Steane, "Quantum Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1701–1703, 1999.